УДК 004.056

Лимарчук-Яциковська Т.О., студентка гр. 125м-16-1,
Науковий керівник: Мілінчук Ю.А., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

Архітектурні методи в кібербезпеці

У наш час більшість підприємств вже замислюється над тим, що їм треба захищати свою інформацію та інформаційні ресурси. В Україні швидкий зріст кількості місць працевлаштування, був зумовлений масивною атакою 27 червня 2017 року. Після нечуваної для України кібератаки, майже всі зрозуміли, що їм треба фахівець з ІБ.

Але, навіть з розумінням, поведінка керівників відрізняється в залежності від рівня розвитку підприємства. У представників великих підприємств (з річним доходом більше суми 50 мільйонів євро та середньою кількістю працівників рівною 250 особам [1]) такі спеціалісти зазвичай включені до складу працівників; у представників малого бізнесу та мікропідприємств (з річним доходом менше суми у 10 мільйонам євро та середньою кількістю працівників не більше 50 осіб [1]) проблеми ІБ не є першочерговими та інформація яка циркулює на підприємстві, частіше за все, коштує менше ніж засоби захисту інформації. А усі інші підприємства, що включені до поняття «середнього підприємства» вже вважають доцільним піклуватись за свою інформацію та ще не знають, що для цього потрібно. Тому вони потребують уваги та великих трудовитрат .

Для вирішення їх завдань може використовуватьcя архітектура підприємства (Enterprise Architecture), що дозволяє сформувати набір принципів, підходів і технологій, які, з огляду на поточний стан організації, закладають основу її подальшої трансформації, зростання і розвитку. Сьогодні існує чимало підходів до створення таких архітектур. Але який би з підходів не був вибраний, в сучасних умовах просто неможливо розвиватися без використання інформації та інформаційних технологій, які повинні не тільки підтримувати будь-які зміни в бізнесі, але і передбачати їх, готуватися до них заздалегідь , а в ряді випадків і сприяти появі нових бізнес-можливостей. Однак не завжди бізнес розвивається передбачуваним чином. Ризики різної природи можуть порушити зростання і розвиток підприємства і поставити його на грань вимирання. Чималу роль в цьому відіграють інформаційні та операційні ризики, пов’язані з витоками даних, виведенням з ладу елементів IT-інфраструктури і т.п. Для того щоб підготувати себе до ризиків сьогодення і майбутнього необхідна архітектура інформаційної безпеки, що пронизує всі інші архітектури підприємства. [2]

Завдяки архітектурному підходу про ІБ тяжче буде забути іншим підрозділам та IT-спеціалісти не нароблять помилок на етапі побудови моделі не питаючись в ІБ-фахівців. Архітектура IT систем підприємства дозволяє побачити усі процеси компанії та побудувати оптимізовані алгоритми роботи різних підрозділів. У чому ж полягає оптимізація? Наприклад, хоча теоретично грамотна розробка архітектури та стратегії повинна здійснюватися зверху вниз (спочатку визначаються цілі, потім способи їх досягнення і тільки потім накуповується різне ПЗ і апаратура, можлива реалізація проектів і т.д.), на практиці ж все зазвичай відбувається навпаки: спочатку здійснюється закупівля «потрібних» засобів захисту, які у всіх на слуху, потім починається їх експлуатація, виявляються недоліки при впровадженні та підтримці, ведеться пошук шляхів оптимізації наявних ресурсів і оцінки ефективності використовуваних технологій і захисних заходів і тільки після цього хтось починає замислюватися про стратегію та архітектуру ІБ.

Другим за поширеністю після відсутності архітектури і стратегії є підхід, що полягає у виробленні бачення або плану застосування технічних рішень або організаційних заходів: аудиту безпеки, підвищення обізнаності, тощо. І хоча це краще, ніж нічого, до розробки реальної архітектури такий підхід не дотягує з двох причин: відсутні цілепокладання і прив'язка до бізнесу та відсутні метрики ефективності досягнення заявлених цілей.

Отже, якщо зрозуміло, що є потреба у комплексному підході та у найбільш щільному «вбудуванні» ІБ в процеси компанії, допоміжним інструментом може стати архітектурний метод будування ІТ-систем, але і його треба дороблятиз огляду на вимоги ІБ. Архітектура ІБ повинна розроблятися зверху вниз, відштовхуючись від цілей та стратегії підприємства, в яких зафіксовано, що і як має бути зроблено в контексті всієї компанії. Архітектура, в свою чергу, присвячена тому, як ці цілі реалізуються з точки зору інформаційної безпеки. Облік стратегії бізнесу дозволяє зрозуміти в цілому, на чому необхідно сконцентруватися в архітектурі ІБ. Якщо перед компанією стоїть завдання географічної експансії та серйозного зростання, то впроваджувані рішення в області інформаційної безпеки повинні сприяти цій меті. Зокрема, велику увагу потрібно приділити VPN-рішень, захищеному віддаленого доступу і т.п. На етапі стабілізації бізнесу акцент зміщується в бік підвищення якості обслуговування, зростання лояльності клієнтів, і інформаційна безпека повинна бути спрямована саме на це. В умовах нестабільної економічної ситуації і бізнес-рішення докорінно змінюються, і система безпеки вже вирішує зовсім інші завдання: захист від витоків і крадіжки інформації з боку співробітників, що звільняються, безпеку аутсорсингу і т.п. Тому потрібно розробляти архітектуру повинні фахівець з інформаційної безпеки та керівник підрозділу ІТ разом, запрошуючи керівників різних підрозділів для розуміння їх потреб та зважати на потреби бізнесу. У такому разі ризики ІБ будуть зменшені, проблеми масштабованості зустрічатися рідше, а рядовий персонал буде більш спокійно реагувати на обмеження висунуті політикою інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лист ДФС від 08.11.2016 № 24033/6/99-99-14-03-03-15
2. Архітектура і стратегія інформаційної безпеки Cisco. https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/Cisco_Security_Architecture.pdf